Cloud Computing Security using Blockchain

Ashok Gupta[1], Shams Tabrez Siddiqui[2], Shadab Alam[3] and Mohammed Shuaib[4]
[1 23 4] Department of Computer Science, Jazan University.

Abstract: Cloud computing has come out as a key technology to deliver infrastructure and data service requirements at low cost and with minimal efforts and high level of scalability and hence have been highly implemented in various aspects of IT industry. A rapid growth in Cloud Computing adaption has been observed but, still, the information security concerns have not been fully countered. Information security concerns are still hindering the growth of Cloud Computing to some extents and need to be resolved. At the same time Blockchain has emerged as a key technology to provide security especially in aspects of integrity, authenticity and confidentiality. This paper reviews the various aspects of security in Blockchain and Cloud Computing and further analyses the application of Blockchain in Cloud Computing security.

IndexTerms **- Cloud Computing, Blockchain, Security, Information security.**

I. INTRODUCTION

Cloud users request for the services from the Cloud Service Providers (CSP). CSPs are third party that providers cloud storage services to their clients. Some other third party service providers are Third-Party Auditor (TPA) and Attribute Authority (AA) that are supposed to provide security functionalities in cloud [1]. As it is known to us that security and trust are the most critical and crucial issues while benefitting the organizations and institutions with cloud. There are a lot of reasons and some of them are [2] [3];

Cloud users data are on high risk which can be lost, leaked or attacked but they do not have any recourse to come out of this substandard situation. Cloud users do not even aware of to whom they are dealing with or sharing data. Transparency is also a very serious, cloud users do not have any information about the users of their data and how the data is roving inside the cloud.

Blockchain is an emerging and novel technology that can be used by cloud users to upsurge the trust and provide security of data while outsourcing and acquiring services from the Cloud. Blockchain can provide advanced security as compared to centralized database security. Blockchain continuously monitors the list of records that are linked and secured using a cryptographic hash function to the previous block [4]. A blockchain is a distributed ledger that can record transactions and prevents tampering. Blockchain typically managed through peer to peer network and designed to disable arbitrary tampering. Blockchain can provide security at par with the data storage at central database. From management aspects, the data storage damages and attacks can be prevented.

Moreover, since the Blockchain has openness attribute, it can provide transparency in data when applied to an area requiring the disclosure of data. Due to such strengths, it can be utilized in diverse areas including the financial sector and the Internet of Things (IoT) environment and its applications are expected to expand [5][6][7][8][9]. Cloud computing has been applied to many IT environments due to its efficiency and availability. Moreover, cloud security and privacy issues have been discussed in terms of important security aspects [10].

II. STRUCTURE OF BLOCKCHAIN

Generally, in Blockchain, a block contains the main data like the hash of current, previous, timestamp and other information. Figure 1 shows the structure of a block [4] [6].

Main data: Normally depending upon the types of the services provided by the block, namely bank transaction records, contact records, clearance records or data records of IoT.

Hash: After the execution of transaction it hash to code and then broadcast to other nodes. Blockchain uses Merkle tree function to reduce the data transmission and computing resources because each node blocks contains thousands of transaction records as well as records the final hash to block header.

Timestamp: Time duration of block generation.

Other Information: Mainly block signature, data that user defines or nonce value are under the categories of other information [11].

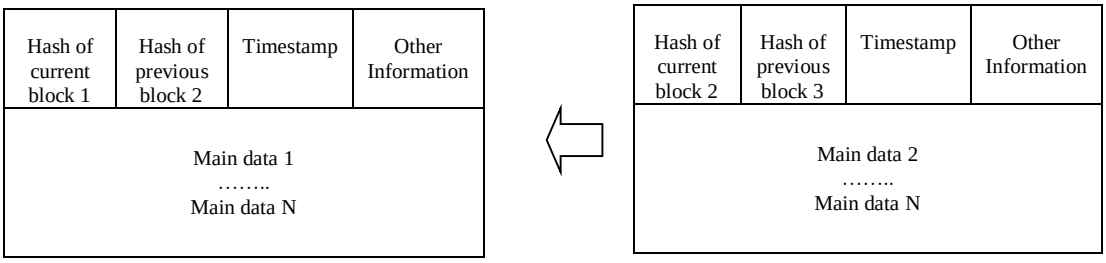

Figure 1: Blockchain structure

As given in table 1, the blockchain block consists of a block body followed by a block header. Block header comprises of Block version, Parent block hash, Merkle tree root hash, Timestamp, n Bits, Nonce value [12]. A block comprises of a header, which encloses metadata of the block details, the key hash of the previous block along with its own key hash, and valid transactions list. 500 transactions contained by a single block and each block is termed the "Block Height". Single transaction average size is 250 bytes but the block header is of 80 bytes [13].

Table 1

Type	Size (in bytes)	Description
Block Size	4	Size of the block
Counter	1-9	No of transactions
Block Header	80	Block header information

III. Characteristics Of Blockchain

Requirements signify all those characteristics and properties that a Blockchain system should acquire and the limitations under which the system should work effectively and efficiently. Hence, they influence the overall functionality of the Blockchain system and can have a larger effect on the system design. Some of the non-functional attributes of the blockchain network are as follows.

- **Openness:** Blockchain has the ability, due to the compatible nature of the nodes, to use and interchange the information during a transaction.
- **Concurrency:** Blockchain performance, as nodes process concurrently, improves.
- **Scalability**: Addition and deletion of new Nodes make Blockchain scalable.
  As far as Scalability is concerned, the focus is majorly on the three parameters:
  - Transaction Processing rate of Distribution:
  - Size:
  - latency or Manageability:
- **Fault tolerance:** The fault-tolerant property of Blockchain network, fault at any node will be transparent to all other nodes in the Blockchain, makes the network to operate properly in case of a fault.
- **Transparency:** The Blockchain transactions are visible to each and every node in the network.
- **Security:** To secure data, powerful Cryptographic protocols are used in the Blockchain network, such as SHA-255.
- **Quality of Service:** Response time and reliability, the time is taken by the transaction to completion and the commitment to deliver the required services, determines the quality of service (QoS) in the Blockchain network.
- **Failure Management:** There must be a process, which can make Blockchain network robust, and can determine the cause of failure. It can suggest how to recover from the failure automatically.

IV. Requirement of Cloud

Some of the important Requirements of Cloud that can influence various design patterns of the Cloud [14][15].

- **Scalability:** Cloud Network handles millions of users or nodes using Cloud services. The hardware architecture is flexible in size, and nodes can be scale in and scale-out.
- **Elasticity:** Proficient Blockchain System can amend workload by allocating and de-allocating resources in a programmed fashion, so that at every point in time all the existing resources meet the current requirements, to the highest feasible level.
- **Privacy:** All users should have effective control over his/her data, and the system should also protect it.
- **Infinite Computing Resources:** The provisioning services from the cloud need not be planned by the users in advance.
- **Pricing:** Different application and services in the Cloud varied in charges and the payment depends on the utilization of the resources.
- **Utilization:** The resources, by allowing the best possible utilizations, can be effectively reconfigured to fine tune the variable load.

- **Cost Efficiency:** Cloud services are need based across the internet, convenient for the end user, as the user is not required to purchase the software licenses which are well suited for the hardware. This will decrease the overall cost of software maintenance and operations.
- **Performance:** In general, Evaluations are quantified in terms of efficiency of the applications and functions running on the cloud system.
- **Flexibility:** The capability of sharing files or services over the internet comes under flexibility. Cloud provides flexibility to a greater extent to the users.

V. Challenges For Blockchain Security

As we know Blockchain technology is directly related to computer-generated and virtual money and used by all users. But, still several Blockchain security challenges are reported, these are as follows:

1. Blockchain Agreement
2. Transactions Security
3. Wallet Security
4. Software Security

5.1 Blockchain Agreement

Blockchain is the collection of sequential connection of fundamental generated blocks, a Blockchain may split into two since temporarily generated last two blocks can be used by two different users, if two distinct peers produced a result during mining at the same time. The block will become insignificant if it's not picked by the peers in the Bitcoin network as the latest block, continuous mining will become pointless. In the Bitcoin peers with more than fifty per cent mining potential will be followed by the network.

5.2 Transaction Security

Various transaction forms can be created using a flexible programming language along with well-written script for inputs and outputs to handle security issues. Bitcoin contract is used for verification, validation and financial services [11] [13]. A most common method to create a contract is based on the script that includes a multiple-signature technique called multisig.

5.3 Wallet Security

Encrypted with a combination of personal and public keys the Bitcoin address uses the hash value of a public key. So, the Bitcoin transaction locking script address cannot be unlocked without an unlocking script that contains the value generated from the combination of a public key and the personal key. Information such as the personal key of the address, which is used for the generation of the unlocking script is stored inside the Bitcoin wallet. That means if we lose information inside the wallet leads to a loss of Bitcoin, as we know to use Bitcoin the information is required and important. Consequently, the Bitcoin wallet turns out to be the prime focus of Bitcoin attack via hacking [16].

5.4 Software Security

Software used in Bitcoin is of major concern, as the bug in the software which is used in Bitcoin can be critical. Although the authorized and certified developer Documentation of Bitcoin apparently explains all related Bitcoin processes; the main software of Bitcoin is still very proficient and effective, as the detailed processes of the initial Bitcoin software have been directed and implemented using the software developed by Satoshi Nakamoto [13][17].

VI. Secure Blockchain Solution For Cloud

In the cloud computing system, if users' confidential data is disclosed, economical and psychological losses can take place due to this leakage in the sensitive data. We mainly study the security of the data while transmitting and saving, such as integrity & privacy, in the cloud computing environment. Blockchain enhanced to an appropriate service level can ensure security, if it's incorporated with the cloud computing environment [18]. While using Blockchain technology, a secure e-wallet is installed. The user information can be misused if the e-wallet is not deleted properly. This remaining data about the user can be used to extract the user information.

Incidences of double transactions of Blockchain and forging the ledger or Bitcoin comes as a major challenge. A safe and reliable e-wallet is required to handle such security issues. Normally the e-wallets installed on the PCs are used, but mobile devices are becoming more popular day by day, so the need of the hour is to verify the security of e-wallets in mobile devices more stringently. Subsequently, a transaction completes only when accuracy and integrity based on the time stamp created in a mobile device, ensure the security of a transaction [17]. A secure e-wallet must be created by reducing, verifying and validating problems that can appear at each step of planning, requirements analysis, implementation and testing, and maintenance.

A secure and reliable restoration of the e-wallet must be incorporated if the security is compromised or hacked by the attackers. It must ensure the security, for the user transaction data saved in the e-wallet and the settings required to manage and operate e-wallet. It must provide a mechanism to remove the remaining user data effectively and securely when the e-wallet is not used and must discard the rest of the data subsequently.

VII. Blockchain Use Cases of Cloud

7.1 Open Ledger

For each and every user, Cloud storage used by Blockchain is accessible and open and can view all sort of services provided by the Cloud including the Service Level Agreements (SLAs). All user can see the level of security, Cloud will deliver and offer. With the level of transparency and open specifications of Cloud, the Cloud users can simply choose and select their required services without making any advance payment.

7.2 Distributed Ledger

All ledger copies are well synchronized, and all cloud users can view the same version/copy of the ledger. The ledger contains the record of services used by individual cloud user and in general service usage, Policies and SLAs. In [19] author states, by utilizing the theory of miners in Bitcoin, Cloud users standardize their ledgers.

7.3 Decentralized Smart Contract

According to [20], in Blockchain a term smart contract, a software that keeps terms and conditions of the contract, verifying the terms and execute the terms, is used. Blockchain coupled with smart contracts technologies enables more trust and transparency on CSP, TPA, AA parties. Smart Contracts are stored on the Blockchain which all cloud users have a copy of it. When the payment is confirmed the service is outsourced. All contract transactions are stored in chronological order on the Blockchain for future access along with the complete audit trail of events. If any party tries to change a contract on the Blockchain all other cloud users can detect and prevent it.

VIII. Conclusion

In this paper, the general structure of Blockchain has been discussed. Further, the characteristics of Blockchain and Cloud Computing security requirements have been analyzed. Based on this analysis, it has been established that Blockchain can be a suitable and powerful tool to provide security in the Cloud Computing environment. Further, this paper reviewed the various existing blockchain implementations for Cloud security.

References

[1] Li, J. Jia, C. Li, J. and Chen, X. 2012. Outsourcing encryption of attribute-based encryption with MapReduce. In: Chim, T.W., Yuen, .H. (eds.) ICICS 2012. LNCS, vol. 7618: 191–201.

[2] Hur, J. and Noh, D.K. 2011. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans. Parallel Distrib. Syst. (TPDS) 22(7): 1214–1221.

[3] Verizon 2015: 2015 Data Breach Investigations Report (2015). http://www.verizonenterprise.com/DBIR/2015/. Accessed 20 Sept 2017

[4] https://en.wikipedia.org/wiki/Blockchain.

[5] Beikverdi, A. and JooSeok. S. 2015. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan.

[6] Bonneau, J. Miller, A. Clark, J. Narayanan, A. Kroll, J.A. and Felten E.W. Sok. 2015. Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA.

[7] Christidis, K. and Michael, D. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4: 2292–2303.

[8] Huang, H. Chen, X. Wu, Q. Huang, X. and Shen. J. 2016. Bitcoin-based fair payments for outsourcing computations of fog devices. Future Gener. Comput. Syst.

[9] Huh, S. Sangrae, C. and Soohyung. K. 2017. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea.

[10] Singh, S. Jeong Y.-S. and Park. J.H. 2016. A survey on cloud computing security: Issues, threats, and solutions. J. Netw. Comput. Appl. 75: 200–222.

[11] Antonopoulos, Andreas M. 2014. Mastering bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc.

[12] Vasek, M. and Moore. T. 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, Springer: Berlin/Heidelberg, Gemany.

[13] Kaskaloglu, K. 2014. Near zero Bitcoin transaction fees cannot last forever. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014), The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic.

[14] Shuaib, M. Samad, A. Alam S., and Siddiqui. S. T. 2019. Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration. Ambient Communications and Computer Systems: Advances in Intelligent Systems and Computing, vol 904. Springer, Singapore: RACCCS-2018, 387.

[15] Shuaib, M. Samad, A. and Siddiqui. S. T. 2017. Multi-layer security analysis of hybrid Cloud. In 6th international conference on system modeling & advancement in research trends, 526-531.

[16] Bamert, T. Decker, C. Wattenhofer, R. and Welten S. 2014. BlueWallet: The Secure BitcoinWallet. In Security and Trust Management; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 65–80.

[17] Haber, S. and Stornetta, W.S.1990. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia.

[18] Alam, S. Siddiqui, S. T. Masoodi, F. and Shuaib M. 2018. Threats to Information Security on Cloud: Implementing Blockchain, 3rd international conference on SMART computing and Informatics (SCI), 21-22 December 2018, Kalinga Institute of Industrial Technology, Odisha. Springer. SPRINGER-SIST series.

[19] Zhang, J. Nian, X. and Xin. H. 2014. A Secure System For Pervasive Social Network-based Healthcare. IEEE Access 2016, 4: 9239–9250.

[20] Omohundro. S. 2014. Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters 1 (2): 19–21.